2

REAL-TIME FAULT TOLERANT COMPUTER SYSTEMS

Contract Number: N00014-92-J-1524

YEARLY REPORT

1 April 1992 - 30 September 1992

Prepared for:

Chief of Naval Research
Code 1133/Annual Report
Ballston Tower One
800 North Quincy Street
Arlington, Virginia 22217-5660

Principal Investigators:

John Lehoczky
Lui Sha
Marc Bodson
Ragunathan Rajkumar
Carnegie Mellon University
Pittsburgh, PA 15213

92 11 06 028

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University

Contract Title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Apr 92 - 30 Sep 92

1 Productivity Measures

This project was initially funded on April 1, 1992 to investigate the use of *analytic redundancy* as an approach to software fault tolerance. This research project is a new part of a larger project at Carnegie Mellon University (the ART Project) which is also funded in part by the Office of Naval Research. The publication productivity measures and the publications listed in this report are those which are associated only with the use of analytic redundance. A more complete report of the activities of the ART Project is contained in the yearly report for ONR Contracts N00014-84-K-0734 and N00014-92-J-1771 and in the 1991 and 1992 *ART Project Briefing* material.

- Papers submitted but not yet accepted: 0
- Refereed papers accepted and in press: 1
- Refereed papers published: 1
- Books submitted or published: 0
- Other reports: 0
- Ph.D. dissertations: 0
- Patents filed or granted: 0
- Invited presentations: 14
- Contributed presentations: 2
- Honors, Prizes and Awards received:
  - **John Lehoczky**:
    - Associate Editor, Journal of *Real-Time Systems*,
    - Member of the program committee of the 12th IEEE Real-Time Systems Symposium, the 8th IEEE Real-Time Operating Systems Workshop, the 11th ICDCS, and the 1992 SIGMETRICS and Performance 92 conferences.
    - Member, NIH Special Study Section on Statistics,
  - **Lui Sha**
    - Member NASA Space Station Advisory Committee,
    - Chairman of the Board of Visitors of RICIS, an R&D center established by NASA and NASA JSC at University of Houston at Clearlake.
    - Program chair, 12th IEEE Real-Time Systems Symposium,
    - General chair, 13th IEEE Real-Time Systems Symposium,
    - Program Committee, 2nd International Workshop on Responsive Systems,

    - Associate Editor, *Real-Time Systems*
    - Associate Editor, *IEEE Computer*
- **Marc Bodson**
    - Program Committee, 1993 Automatic Control Conference
    - Member National Science Foundation Review Panel on robust, adaptive and nonlinear control.
    - Elected to Board of Directors, IEEE Pittsburgh Chapter, 1992-1993
    - Co-chairman IEEE Control System Society Pittsburgh Chapter, 1991-1992.

- Graduate students supported: 1 (Jennifer M. Stephan)
- Undergraduate students supported: 3, (W. Mark Smith, Charles W. Hewgley and Wai Kok)
- Post-docs supported: 0
- Minorities supported: 0
- Women supported: 1 graduate student

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University

Contract Title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Apr 92 - 30 Sep 92

2 Summary of Technical Progress

2.1 Overview of Technical Approach

This research project is developing a new approach to software fault tolerance called analytic redundancy. It has been widely acknowledged that software failures are the most important issue in large computer system reliability. The failure rate of software has risen to 9.4 times the failure rate of hardware, and software failures have captured substantial media attention in recent years. The problem of software reliability is especially difficult because the major recognized approaches (recovery blocks and n-version programming) are known to have serious drawbacks.

Analytic redundancy is an approach which uses simplicity (in the form of software which is relatively simple, well understood and well tested but whose performance is merely adequate) to control complexity (in the form of software which has high performance but is complex and, therefore, not reliable). Rather than trying to combine the two algorithms (which would create an even less reliable system), we allow the complex software to control the system as long as it is behaving properly (as judged by the simple software). If it is determined that the complex software is behaving incorrectly, then the simple software takes over. The simple software will guarantee a baseline, if not optimal, performance.

We are considering two classes of examples: (1) control systems and (2) tracking systems, and we are addressing both by developing an appropriate theory and experimental prototypes. In each case, we are developing a set of algorithms which span the range of complexity and functionality. The major research challenge is to determine conditions under which the complex algorithm is behaving erroneously and then to execute a switch in control from the complex to the simple. These two classes of problems are discussed below.

2.2 Control System Example

A laboratory experiment consisting of a ball rolling freely on a rotating beam was constructed. The angle of the beam is controlled through an electric motor, and the position of the ball is measured through a resistive wire placed on the beam. Our plan calls for the base of the experimental apparatus to also rotate; however, this has not yet been implemented.

Several papers from the recent control theory literature were studied. A dynamic model of the system was obtained to be used as the basis for computer simulations of the system. The system was found to be highly unstable, a property which makes it perfectly suited for our purposes. A range of possible control strategies were considered for this problem. At this point, we designed a simple p.i.d. (proportional integral derivative) controller, and a more complex adaptive algorithm. We introduced the possibility of two sizes of balls being used. The adaptive algorithm is capable of maximizing system performance without knowledge of the size of the ball actually being controlled.

We have studied the design of a switching strategy to recover stability if the adaptive algorithm were to fail. It was found that the algorithm becomes unstable in certain regions of the state space for an important range of parameter values.

In the near future, we plan to complete the design and testing of the algorithms, including the switching logic, so that a first demonstration of the principal ideas of the proposal will be available soon. We also plan to develop formal design procedures based on the experience gained in this example.

2.3 Airborne Radar Systems

There are several distinct algorithmic approaches that can be used by airbome radar tracking systems. These include nearest neighbor algorithm, Joint Probabilistic Data Association (JPDA) and multiple hypothesis testing. Each approach has it strengths and weaknesses in terms of its performance, computational complexity and failure characteristics. While there is a large literature on the optimality of certain tracking algorithms, only nearest-neighbors-based algorithms have been fielded. The technology is well understood, and there is great hesitancy to introduce higher performance approaches because of the potential for faulty software. Thus this application is well suited to using analytic redundancy, because this technique holds the promise of permitting the introduction of sophisticated software offering great functionality while controlling the risks from faults associated with the greater complexity.

We are exploring the application of these ideas with MITRE. We are considering using different algorithms in different circumstances, and when sophisticated algorithms are used, we will allow the simple algorithms to determine if the complex software is failing. The problem is challenging, but the approach is promising. Moreover, because of the involvement of MITRE, we will be able to implement and test our ideas in a simulation testbed. Eventually, these ideas will be integrated into the rate monotonic theory to handle the real-time aspects of the problem. Substantial progress is expected during the next year.

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract Title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Apr 92 - 30 Sep 92

3 Publications

3.1 Published or In Press

- Sha, L., Lehoczky, J. and Bodson, M., "The simplex architecture: Analytic redundancy for software fault tolerance," *Proceedings of the 1st International Workshop on Responsive Computer Systems*, Nice, France, October 1991.
- Sha, L., Lehoczky, J., Bodson, M., Krupp, P. and Nowacki, C., "Responsive airborne radar systems," to appear in *Proceedings of the Second International Workshop on Responsive Systems*, 1992.

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University
Contract Title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Apr 92 - 30 Sep 92

4 Transitions and DoD Interactions

We have been interacting with MITRE Corporation to investigate the application of analytic redundancy to airborne radar systems. The application is very promising and is being implemented by the CMU Software Engineering Institute (by L. Sha and R. Rajkumar of the SEI's ZDAK Project) and MITRE.

Principal Investigator Names:

J. Lehoczky	(412) 268-8725	jpl@k.cs.cmu.edu
L. Sha	(412) 268-5875	lrs@sei.cmu.edu
M. Bodson	(412) 268-3898	bodson@galley.ece.cmu.edu
R. Rajkumar	(412) 268-8707	rr@sei.cmu.edu

PI Institution: Carnegie Mellon University

Contract Title: Real-Time Fault Tolerant Computer Systems
Contract Number: N00014-92-J-1524
Reporting Period: 1 Apr 92 - 30 Sep 92

5 Software and Hardware Prototypes

An important part of this project is laboratory experimentation to empirically test the analytic redundancy approach to fault tolerance. Hardware and software prototypes are being developed for the ball and beam control experiment. In addition, we are cooperating with MITRE Corporation and the CMU Software Engineering Institute in developing a software prototype demonstrating the use of analytic redundancy for enhancing the fault tolerance of the tracking systems used in airborne radar systems.